EXAMINER'S AMENDMENT

CANCEL:

Claim 28, 33, and 45.

AMEND:

Claim 31 should be dependent on independent claim 27

Claim 36 should be dependent on independent claim 32

REPLACE:

Claims 27, 32, and 37-43 with the Claim limitations below:

27. (currently amended) A signing apparatus, including a processor, used in an authentication system which uses authentication data created by applying one-way functions to information divisible into a plurality of data divisions thereof, the apparatus comprising:

a dividing unit which divides the information into the plurality of data divisions;

an authenticator creating unit which creates a first authenticator by applying a first one-way function using a first key to all of the data divisions, and creates a second authenticator by applying a second one-way function using a second key to each all of the data divisions, where the first and second keys are different; and

an appending unit which links the first and second authenticators, and appends linked authenticators to the information for sending with the information to a certifying apparatus in the

authentication system,

wherein the dividing unit divides the information into the plurality of data divisions including a first data division and a second data division, each having a pre-specified length, and

the authenticator creating unit creates the first authenticator by applying the first one-way function using the first key to a first initial value and one of the data divisions to obtain a first result and by applying the first one-way function using the first key to the first result obtained by previous application of the first one-way function and each of the other data divisions respectively, and creates the second authenticator by applying the second one-way function using the second key to a second initial value and the first one of the data divisions to obtain a second result and by applying the second one-way function using the second key to the second result obtained by previous application of the second one-way function and each of the other data divisions respectively.

32. (currently amended) A certifying apparatus, including a processor, used in an authentication system which uses authentication data created by applying one-way functions to information divisible into a plurality of data divisions, the apparatus comprising:

a separating unit which separates out the information and linked authenticators from authenticator-appended information which is received from a signing apparatus in the authentication system;

a dividing unit which divides the information separated out by the separating unit into the plurality of data divisions;

an authenticator creating unit which creates a first authenticator by applying a first one-way function using a first key to all of the data divisions, and creates a second authenticator by applying a second one-way function using a second key to all of the data divisions, where the first and second keys are different; and

a certifying unit which authenticates the information by comparing the first authenticator with a third authenticator of the linked authenticators separated out by the separating unit, and by comparing the second authenticator with a fourth authenticator of the linked authenticators separated out by the separating unit, wherein

the dividing unit divides the information separated out by the separating unit into the

plurality of data divisions including a first data division and a second data division, each having a pre-specified length, and

the authenticator creating unit creates the first authenticator by applying the first one-way function using the first key to a first initial value and one of the data divisions to obtain a first result and by applying the first one-way function using the first key to the first result obtained by previous application of the first one-way function and each of the other data divisions respectively, and creates the second authenticator by applying the second one-way function using the second key to a second initial value and one of the data divisions to obtain a second result and by applying the second one-way function using the second key to the second result obtained by previous application of the second one-way function and each of the other data divisions respectively.

37. (currently amended) A signing method used in an authentication system which uses authentication data created by applying one-way functions to information divisible into a plurality of data divisions, the method comprising:

dividing the information into the plurality of data divisions;

creating a first authenticator by applying a first one-way function using a first key to all of the data divisions;

creating a second authenticator by applying a second one-way function using a second key to all of the data divisions, where the first and second keys are different; and

appending linked authenticators, the linked authenticators being obtained by linking the first and second authenticators, to the information for sending with the information to a certifying apparatus in the authentication system,

wherein the dividing the information into the plurality of data divisions including a first data division and a second data division, each having a pre-specified length, and

wherein the creating the first authenticator by applying the first one-way function using the first key to a first initial value and one of the data divisions to obtain a first result and by applying the first one-way function using the first key to the first result obtained by previous application of the first one-way function and each of the other data divisions respectively, and creates the second authenticator by applying the second one-way function using the second key

to a second initial value and the first one of the data divisions to obtain a second result and by applying the second one-way function using the second key to the second result obtained by previous application of the second one-way function and each of the other data divisions respectively.

38. (currently amended) A certifying method used in an authentication system which uses authentication data created by applying one-way functions to information divisible into a plurality of data divisions, the method comp rising:

separating out the information and linked authenticators from authenticator-appended information which is received from a signing apparatus in the authentication system;

dividing the separated out information into the plurality of data divisions;

creating a first authenticator by applying a first one-way function using a first key to all of the data divisions;

creating a second authenticator by applying a second one-way function using a second key to all of the data divisions, where the first and second keys are different; and

authenticating the information by comparing the first authenticator with a third authenticator of the linked authenticators, and by comparing the second authenticator with a fourth authenticator of the linked authenticators,

wherein the dividing the information into the plurality of data divisions including a first data division and a second data division, each having a pre-specified length, and

wherein the creating the first authenticator by applying the first one-way function using the first key to a first initial value and one of the data divisions to obtain a first result and by applying the first one-way function using the first key to the first result obtained by previous application of the first one-way function and each of the other data divisions respectively, and creates the second authenticator by applying the second one-way function using the second key to a second initial value and the first one of the data divisions to obtain a second result and by applying the second one-way function using the second key to the second result obtained by previous application of the second one-way function and each of the other data divisions respectively.

39. (currently amended) A computer program product stored on computer readable medium for signing in an authentication system which uses authentication data created by applying one-way functions to information divisible into a plurality of data divisions, the computer program product including computer executable instructions stored on a computer readable medium, wherein the instructions, when executed by a computer, cause a computer to perform a process, the process comprising:

dividing the information into the plurality of data divisions;

creating a first authenticator by applying a first one-way function using a first key to all of the data divisions;

creating a second authenticator by applying a second one-way function using a second key to all of the data divisions, where the first and second keys are different; and

appending linked authenticators, the linked authenticators being obtained by linking the first and second authenticators, to the information for sending with the information to a certifying apparatus in the authentication system,

wherein the dividing the information into the plurality of data divisions including a first data division and a second data division, each having a pre-specified length, and

wherein the creating the first authenticator by applying the first one-way function using the first key to a first initial value and one of the data divisions to obtain a first result and by applying the first one-way function using the first key to the first result obtained by previous application of the first one-way function and each of the other data divisions respectively, and creates the second authenticator by applying the second one-way function using the second key to a second initial value and the first one of the data divisions to obtain a second result and by applying the second one-way function using the second key to the second result obtained by previous application of the second one-way function and each of the other data divisions respectively.

40. (currently amended) A computer program product stored on computer readable medium for certifying in an authentication system which uses authentication data created by applying one-way functions to information divisible into a plurality of data divisions, the computer program product including computer executable instructions stored on a computer

readable medium, wherein the instructions, when executed by a computer, cause a computer to perform a process, the process comprising:

separating out the information and linked authenticators from authenticator-appended information received from a signing apparatus in the authentication system;

dividing the separated out information into the plurality of data divisions;

creating a first authenticator by applying a first one-way function using a first key to all of the data divisions;

creating a second authenticator by applying a second one-way function using a second key to all of the data divisions, where the first and second keys are different; and

authenticating the information by comparing the first authenticator with a third authenticator of the linked authenticators, and by comparing the second authenticator with a fourth authenticator of the linked authenticators,

wherein the dividing the information into the plurality of data divisions including a first data division and a second data division, each having a pre-specified length, and

wherein the creating the first authenticator by applying the first one-way function using the first key to a first initial value and one of the data divisions to obtain a first result and by applying the first one-way function using the first key to the first result obtained by previous application of the first one-way function and each of the other data divisions respectively, and creates the second authenticator by applying the second one-way function using the second key to a second initial value and the first one of the data divisions to obtain a second result and by applying the second one-way function using the second key to the second result obtained by previous application of the second one-way function and each of the other data divisions respectively.

41. (currently amended) An authentication system, including a processor, using authentication data created by applying one-way functions to information divisible into a plurality of data divisions, the system comprising:

a signing apparatus which includes

a first dividing unit which divides the information into the plurality of data divisions;

an authenticator creating unit which creates a first authenticator by applying a first one-

way function using a first key to all of the data divisions, and which creates a second authenticator by applying a second one-way function using a second key to all of the data divisions, where the first and second keys are different; and

an appending unit which links the first and second authenticators, and appends the linked authenticators to the information for sending with the information to a certifying apparatus in the authentication system; and

a certifying apparatus which includes

a separating unit which separates out the information and linked-authenticators from the authenticator-appended information which is received from the signing apparatus in the authentication system;

a second dividing unit which divides the information separated out by the separating unit into the plurality of data divisions;

an authenticator creating unit which creates a first authenticator by applying a first one-way function using a first key to all of the data divisions, and creates a second authenticator by applying a second one-way function using a second key to all of the data divisions, where the first and second keys are different; and

a certifying unit which authenticates the information by comparing the first authenticator with a third authenticator of the linked authenticators separated by the separating unit, and by comparing the second authenticator with a fourth authenticator of the linked authenticators separated by the separating unit,

wherein the dividing the information into the plurality of data divisions including a first data division and a second data division, each having a pre-specified length, and

wherein the creating the first authenticator by applying the first one-way function using the first key to a first initial value and one of the data divisions to obtain a first result and by applying the first one-way function using the first key to the first result obtained by previous application of the first one-way function and each of the other data divisions respectively, and creates the second authenticator by applying the second one-way function using the second key to a second initial value and the first one of the data divisions to obtain a second result and by applying the second one-way function using the second key to the second result obtained by previous application of the second one-way function and each of the other data divisions

respectively.

42. (currently amended) An authentication method used in an authentication system which uses authentication data created by applying one-way functions to information divisible into a plurality of data divisions, the method comprising:

dividing the information into the plurality of data divisions;

creating a first authenticator by applying a first one-way function using a first key to all of the data divisions;

creating a second authenticator by applying a second one-way function using a second key to all of the data divisions, where the first and second keys are different;

appending linked authenticators, the linked authenticators being obtained by linking the first and second authenticators, to the information for sending with the information to a certifying apparatus in the authentication system;

sending the authenticator-appended information;

receiving and separating out the information and linked authenticators from the sent authenticator-appended information;

dividing the separated-out information into the plurality of data divisions;

creating a first authenticator by applying a first one-way function using a first key to all of the data divisions;

creating a second authenticator by applying a second one-way function using a second key to all of the data divisions, where the first and second keys are different; and

authenticating the information by comparing the first authenticator with a third authenticator, of the linked authenticators, and by comparing the second authenticator with a fourth authenticator of the linked authenticators,

wherein the dividing the information into the plurality of data divisions including a first data division and a second data division, each having a pre-specified length, and

wherein the creating the first authenticator by applying the first one-way function using the first key to a first initial value and one of the data divisions to obtain a first result and by applying the first one-way function using the first key to the first result obtained by previous application of the first one-way function and each of the other data divisions respectively, and

creates the second authenticator by applying the second one-way function using the second key to a second initial value and the first one of the data divisions to obtain a second result and by applying the second one-way function using the second key to the second result obtained by previous application of the second one-way function and each of the other data divisions respectively.

43. (currently amended) A computer program product stored on computer readable medium for authentication in an authentication system which uses authentication data created by applying one-way functions to information divisible into a plurality of data divisions, the computer program product including computer executable instructions stored on a computer readable medium, wherein the instructions, when executed by a computer, cause a computer to perform a process, the process comprising:

dividing the information into the plurality of data divisions;

creating a first authenticator by applying a first one-way function using a first key to all of the data divisions;

creating a second authenticator by applying a second one-way function using a second key to all of the data divisions, where the first and second keys are different;

appending linked authenticators, the linked authenticators being obtained by linking the first and second authenticators, to the information for sending with the information to a certifying apparatus in the authentication system;

sending the authenticator-appended information;

receiving and separating out the information and linked authenticators from the sent authenticator-appended information;

dividing the separated-out information into the plurality of data divisions;

creating a first authenticator by applying a first one-way function using a first key to all of the data divisions;

creating a second authenticator by applying a second one-way function using a second key to all of the data divisions, where the first and second keys are different;

authenticating the information by comparing the first authenticator with a third authenticator, of the linked authenticators, and by comparing the second authenticator with a

fourth authenticator of the linked authenticators,

wherein the dividing the information into the plurality of data divisions including a first data division and a second data division, each having a pre-specified length, and

wherein the creating the first authenticator by applying the first one-way function using the first key to a first initial value and one of the data divisions to obtain a first result and by applying the first one-way function using the first key to the first result obtained by previous application of the first one-way function and each of the other data divisions respectively, and creates the second authenticator by applying the second one-way function using the second key to a second initial value and the first one of the data divisions to obtain a second result and by applying the second one-way function using the second key to the second result obtained by previous application of the second one-way function and each of the other data divisions respectively.

Allowable Subject Matter

The following is an examiner's statement of reasons for allowance: Claims are allowable over the prior art following the agreement by the attorney to amend independent claims with limitations that overcome the prior art of record. These limitations are shown on the record as amended claims 28, and 33.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHRISTOPHER J. BROWN whose telephone number is (571)272-3833. The examiner can normally be reached on 8:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571)272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christopher J Brown/ 6/5/08
Primary Examiner, Art Unit 2134